RADIUSサーバを使用するVPN 3000 Concentrator グループにユーザをロックする方法

目次

概要

Cisco VPN 3000 コンセントレータには、ユーザをコンセントレータ グループにロックする機能があります。コンセントレータ グループは、Cisco VPN 3000 クライアントでユーザが設定したグループをオーバーライドします。 このように、VPN コンセントレータで設定されているさまざまなグループにアクセス制限を適用できます。これによりユーザが RADIUS サーバでそのグループにロックされることが保証されます。

このドキュメントでは、Cisco Secure ACS for Windows および Cisco Secure for UNIX（CSUnix）でのこの機能のセットアップ方法の詳細を説明します。

VPN コンセントレータの設定は標準設定に似ています。 VPN コンセントレータで定義されているグループにユーザをロックできる機能は、RADIUS ユーザ プロファイルで戻り属性を定義することで有効になります。 この属性には、ユーザをロックする VPN コンセントレータ グループの名前が含まれています。 この属性は、Class 属性（IETF RADIUS 属性番号 25）であり、VPN コンセントレータに次の形式で戻される必要があります。

```
OU=groupname;
```

groupname は、ユーザがロックされる VPN コンセントレータのグループの名前です。 *OU* は大文字でなければならず、末尾にセミコロンが必要です。

この例では、VPN Client ソフトウェアが、*グループ名*「Everyone」とパスワード「Anything」が設定されている既存の接続プロファイルを使用して、すべてのユーザに配布されます。 各ユーザにはそれぞれ個別のユーザ名とパスワードがあります（この例では、ユーザ名/パスワードは

TEST/TEST です）。 ユーザ名が RADIUS サーバに送信されると、RADIUS サーバはそのユーザが含まれる*実際のグループ*の情報を送信します。 この例ではこれは「filtergroup」です。

これにより、RADIUS サーバでのグループ割り当てを完全に制御でき、ユーザはこの制御を意識しません。 RADIUS サーバがユーザにグループを割り当てない場合、そのユーザは「Everyone」グループに残ります。 「Everyone」グループに含まれているフィルタは制限が非常に厳しいため、ユーザはどのトラフィックも渡すことができません。 RADIUS サーバがユーザにグループを割り当てる場合、ユーザはそのグループ固有の属性（制限が緩いフィルタなど）を継承します。 この例では、VPN コンセントレータのグループ「filtergroup」に対し、すべてのトラフィックを許可するフィルタを適用します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

注: これは、ACS 3.3、VPN コンセントレータ 4.1.7 および VPN Client 4.0.5 でもテストが完了しています。

- Cisco VPN 3000 コンセントレータ シリーズ バージョン 4.0(1)Rel
- Cisco VPN Client バージョン 4.0(1)Rel
- Cisco Secure ACS for Windows バージョン 2.4 ~ 3.2
- Cisco Secure for UNIX バージョン 2.3、2.5、および 2.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco VPN 3000 コンセントレータの設定

注: この設定では、IP アドレス、デフォルト ゲートウェイ、アドレス プールなどを使用して VPN コンセントレータがすでに設定されていることを前提としています。 ユーザは続行する前に、ローカルで認証できる必要があります。 認証できない場合、これらの変更は機能しません。

1. [Configuration] > [System] > [Servers] > [Authentication] で、RADIUS サーバの IP アドレスを追加します。
2. サーバを追加したら、**[Test] ボタン**を使用してユーザを適切に認証できることを確認します。認証できない場合は、グループ ロックが機能しません。
3. 内部ネットワーク上のすべてのアイテムへのアクセスを削除するフィルタを定義します。こ

れは「Everyone」グループに適用されるため、ユーザが認証されこのグループに追加されても、すべてのデータにアクセスできません。

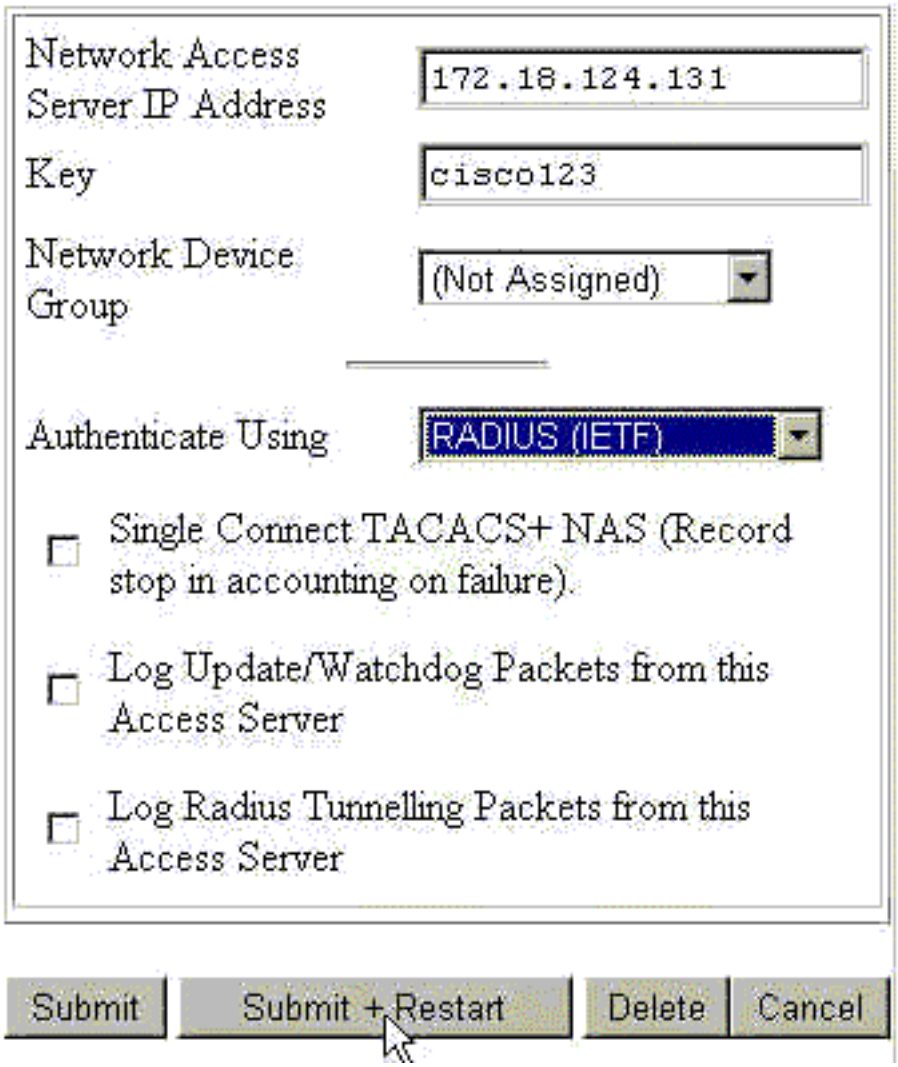
4. **[Configuration] > [Policy Management] > [Traffic Management] > [Rules]** で **Drop All** というルールを追加し、すべてデフォルト設定のままにします。
5. **[Configuration] > [Policy Management] > [Traffic Management] > [Filters]** で **Drop All**という名前のフィルタを作成し、すべてデフォルト設定のままにし、「Drop All」ルールを追加します。
6. **[Configuration] > [User Management] > [Groups]** で **Everyone** という名前のグループを追加します。これは、VPN Client ですべてのユーザに対して事前に設定されているグループです。 ユーザは最初にこのグループに対して認証され、ユーザ認証の完了後に別のグループにロックされます。 通常の方法でグループを定義します。 [General] タブで（作成した）[Drop All] フィルタを追加してください。 このグループのユーザに RADIUS 認証を使用するため、グループの [Type]（[Identity] タブ）を [Internal] に設定し、[Authentication]（[IPSec] タブ）を [RADIUS] に設定します。 このグループに対して [Group Lock] 機能がオンになっていないことを確認します。**注:** [Drop All] フィルタを定義していない場合でも、少なくとも 1 つのフィルタが定義されていることを確認してください。
7. ユーザの最終宛先グループ（例：「filtergroup」）を定義し、フィルタを適用します。**注:** ここでフィルタを定義する必要があります。 これらのユーザに対しトラフィックをすべてブロックしない場合は、「Allow All」フィルタを作成し、[Any In] ルールと [Any Out] ルールをこのフィルタに適用します。 トラフィックを渡すため、なんらかのフィルタを定義する必要があります。 このグループのユーザに RADIUS 認証を使用するため、グループの [Type]（[Identity] タブ）を [Internal] に設定し、[Authentication]（[IPSec] タブ）を [RADIUS] に設定します。 このグループに対して [Group Lock] 機能がオンになっていないことを確認します。

RADIUS サーバの設定

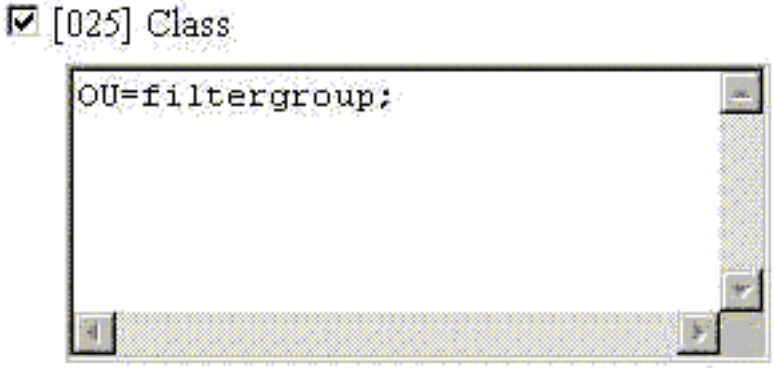
Cisco Secure ACS for Windows

次に示す手順では、RADIUS サーバで Cisco Secure ACS for Windows を設定し、VPN コンセントレータで設定されている特定のグループにユーザをロックします。 RADIUS サーバで定義されるグループは、VPN コンセントレータで定義されるグループにはまったく関係ない点に注意してください。 RADIUS サーバでグループを使用すると、ユーザを容易に管理できます。 名前は、VPN コンセントレータで設定されている名前と一致している必要はありません。

1. [Network Configuration] セクションで、RADIUS サーバのネットワーク アクセス サーバ（NAS）として VPN コンセントレータを追加します。[NAS IP Address] ボックスに、VPN コンセントレータの IP アドレスを追加します。以前に VPN コンセントレータで定義したキーを [Key] ボックスに追加します。[Authenticate Using] ドロップダウン メニューで、[RADIUS (IETF)] を選択します。[Submit + Restart] をクリックします。



2. [Interface Configuration] で [RADIUS (IETF)] を選択し、属性 [25 (Class)] がオンになっていることを確認します。これにより、グループ/ユーザ設定でこの属性を変更できるようになります。
3. ユーザを追加します。次の例では、ユーザは「TEST」です。 このユーザは、任意の Cisco Secure ACS for Windows グループに追加できます。 属性 25 を渡して VPN コンセントレータに対しユーザに使用するグループを指示する操作の他に、Cisco Secure ACS for Windows のグループと VPN コンセントレータのグループの間に相関関係はありません。 このユーザは「Group_1」に追加されます。
4. [Group Setup] で、グループ (例では「Group_1」) の設定を編集します。
5. 緑色の [IETF RADIUS] ボタンをクリックし、該当する属性を表示します。
6. 下へスクロールして、属性 25 を変更します。
7. この属性を次に示すように追加します。 filtergroup を、ユーザをロックするグループの名前に置き換えます。OU が大文字であり、グループ名の後にセミコロンがあることを確認します。

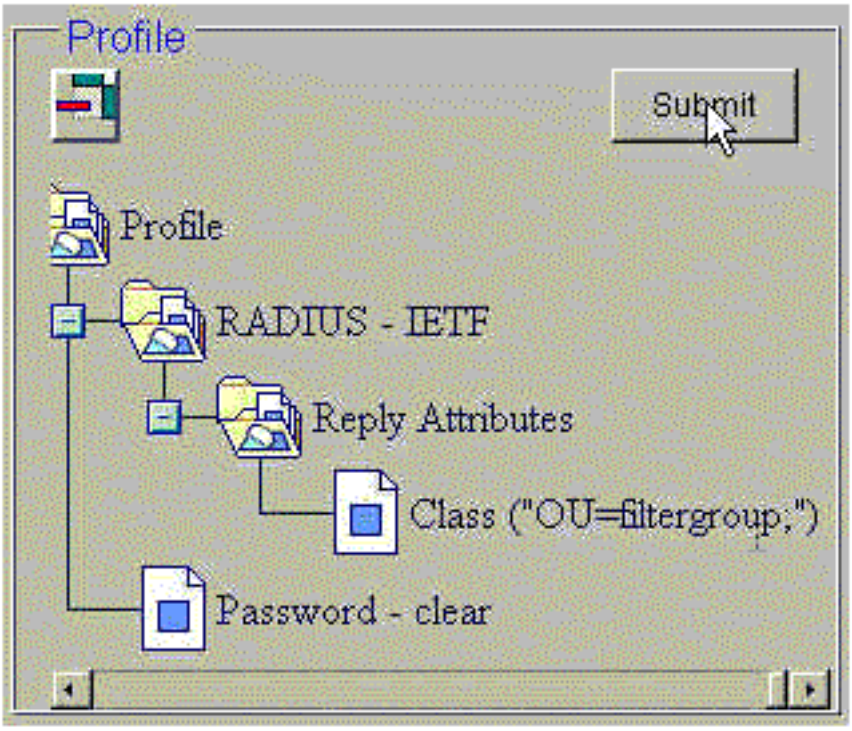


8. [Submit + Restart] をクリックします。

Cisco Secure for UNIX

次に示す手順では、RADIUS サーバで Cisco Secure UNIX を設定し、VPN コンセントレータで設定されている特定のグループにユーザをロックします。 RADIUS サーバで定義されるグループは、VPN コンセントレータで定義されるグループにはまったく関係ない点に注意してください。 RADIUS サーバでグループを使用すると、ユーザを容易に管理できます。 名前は、VPN コンセントレータで設定されている名前と一致している必要はありません。

1. [Advanced] セクションで、VPN コンセントレータを RADIUS サーバの NAS として追加します。属性 25 を reply-attribute として送信できるようにするディクショナリを選択します。 たとえば [IETF] または [Ascend] です。
2. ユーザを追加します。この例では、ユーザは「TEST」です。 このユーザは Cisco Secure UNIX グループに追加するか、またはどのグループにも追加しないでおくことができます。 属性 25 を渡して VPN コンセントレータに対しユーザに使用するグループを指示する操作の他に、Cisco Secure UNIX のグループと VPN コンセントレータのグループの間に相関関係はありません。
3. ユーザ/グループ プロファイルで RADIUS (IETF) 戻り属性を定義します。
4. Class 属性、属性番号 **25** を追加し、その値を **OU=filtergroup;** に設定します。 filtergroup を VPN コンセントレータで定義されているグループに置き換えます。**注:** Cisco Secure UNIX では、属性を引用符で囲んで定義します。 この引用符は、属性を VPN コンセントレータに送信するときに削除されます。 ユーザ/グループ プロファイルは次のようになります。



5. [Submit] をクリックして各エントリを保存します。完了した Cisco Secure UNIX エントリは次の出力のようになります。`# ./ViewProfile -p 9900 -u NAS.172.18.124.132`

```
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
```

```
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- VPN 3000 コンセントレータで処理する際の Cisco VPN 3000 クライアントユーザおよびグループ属性
- RADIUS（Remote Authentication Dial-In User Service）テクノロジーに関するサポート ページ
- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 Client に関するサポートページ
- IP Security Protocol（IPSec）製品に関するサポート ページ
- Requests for Comments（RFC）
- Cisco Secure ACS for Windows 製品に関するサポートページ
- セキュリティ製品に関する Field Notice
- Cisco Secure ACS for UNIX 製品に関するサポートページ
- テクニカルサポート - Cisco Systems